UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/618,861	07/14/2003	Eric Balard	TI-34921	6971

23494 7590 09/09/2010

TEXAS INSTRUMENTS INCORPORATED
P O BOX 655474, M/S 3999
DALLAS, TX 75265

EXAMINER	
LANIER, BENJAMIN E	

ART UNIT	PAPER NUMBER
2432	

NOTIFICATION DATE	DELIVERY MODE
09/09/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

uspto@ti.com

Office Action Summary	Application No.	Applicant(s)	
	10/618,861	BALARD ET AL.	
	Examiner	Art Unit	
	BENJAMIN E. LANIER	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 July 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,4,7,11,14,16,18,19,25,27,29-31,33,35,36,41,42,44 and 46* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,4,7,11,14,16,18,19,25,27,29-31,33,35,36,41,42,44 and 46* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114 was filed in this application after a decision by the Board of Patent Appeals and Interferences, but before the filing of a Notice of Appeal to the Court of Appeals for the Federal Circuit or the commencement of a civil action. Since this application is eligible for continued examination under 37 CFR 1.114 and the fee set forth in 37 CFR 1.17(e) has been timely paid, the appeal has been withdrawn pursuant to 37 CFR 1.114 and prosecution in this application has been reopened pursuant to 37 CFR 1.114. Applicant's submission filed on 26 July 2010 has been entered.

Response to Amendment

2. Applicant's amendment filed 26 July 2010 amends claims 1, 7, 16, 25, 27, 33, and 44. Applicant's amendment has been fully considered and entered.

Response to Arguments

3. Applicant's arguments with respect to the amended claim language have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Zuk, U.S. Patent No. 5,745,571.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

6. Claims 1, 4, 7, 11, 16, 18, 19, 27, 30, 33, 35, 36, 41, 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gray, U.S. Patent No. 6,268,788, in view of Zuk, U.S. Patent No. 5,745,571. Referring to claim 1, Gray (Column 5, lines 62- Column 6, lines 20) & (Column 6, lines 55-Column 7, line 10) & Figure 4 discloses a method of securing access to resources in a computing device, comprising the steps of:

- Generating a random number, using the random number to generate an encrypted access code (Col. 12, lines 6-13)
- Storing the encrypted access code in a memory location within the computing device; (Figure 2 & Column 5, lines 62- Column 6, lines 20) & (Column 6, lines 55-Column 7, line 10)
- Receiving a password to access the resources; (Column 5, lines 62- Column 6, lines 20) & (Column 6, lines 55-Column 7, line 10)
- Encrypting the password to produce the encrypted access code; (Column 5, lines 62-Column 6, lines 20) & (Column 6, lines 55-Column 7, line 10)
- Allowing access to the resources if the encrypted access code matches the encrypted password. (Column 6, lines 16-20) & (Column 6, line 65- Column 7, line 5)

Gray does not disclose that the random keys are generated at the time of manufacturer such that the keys are not known to anyone. Zuk discloses the internal generation of an encryption key at the time of manufacture such that the key is not known to anyone (Col. 5, lines 42-48), which meets the limitation of generating on-chip during production of the computing device, such that the value of the random number generated on-chip is not known to anyone, storing said random number in permanent memory in the computing device. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the random keys of Gray to be generated at the time of manufacture in the manner discussed in Zuk in order to provide secrecy for the key without providing access to the manufacturer as taught by Zuk (Col. 1, lines 22-25 & Col. 5, lines 46-48).

In reference to claim 4:

Gray (Column 5, lines 62- Column 6, lines 20) & (Column 9, lines 53-65) discloses the method of claim 1 wherein the encrypted access code is stored in a memory that cannot be externally modified, where the information stored on the computer system cannot be captured or tampered with and is stored in a secure room.

In reference to claim 7:

Gray (Column 5, lines 62- Column 6, lines 20) & (Column 6, lines 55-Column 7, line 10) & Figures 2, 4 discloses a computing device comprising:

- Generating a random number, using the random number to generate an encrypted access code (Col. 12, lines 6-13)

- A processing system (Figure 2, Items 40 and Items 60)
- A memory coupled to the processing system for storing an encrypted access code; (Figure 2, Items 42 and Items 62)
- Input circuitry coupled to the processing system for receiving a password to access resources; (Figure 2, Items 16 and Items 34)
- Wherein the processing circuitry:
    - Encrypts the password to produce a encrypted password; (Column 6, lines 1-8) & (Column 6, lines 55-Column 7, line 10)
    - Compares the encrypted password to the encrypted access code; (Column 6, lines 1-8) & (Column 6, lines 55-Column 7, line 10)
    - Allows access to the resources if the encrypted access code matches the encrypted (Column 6, lines 55-Column 7, line 10)

Gray does not disclose that the random keys are generated at the time of manufacturer such that the keys are not known to anyone. Zuk discloses the internal generation of an encryption key at the time of manufacture such that the key is not known to anyone (Col. 5, lines 42-48), which meets the limitation of generating on-chip during production of the computing device, such that the value of the random number generated on-chip is not known to anyone, storing said random number in permanent memory in the computing device. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the random keys of Gray to be generated at the time of manufacture in the manner discussed in Zuk in order to provide secrecy for the key without providing access to the manufacturer as taught by Zuk (Col. 1, lines 22-25 & Col. 5, lines 46-48).

In reference to claim 11:

Gray (Column 6, lines 55-Column 7, line 10) discloses the computing device of claim 7 wherein the processing system allows access to testing resources if the encrypted access code matches the encrypted password.

In reference to claims 16, 18, 33, 35:

Gray discloses that the memory can include a ROM (Figure 2, 64), which meets the limitation of the permanent memory comprises a memory array in which after data is written to the array, further writing to the particular memory location is disabled, such that the data cannot be overwritten, a read only memory (ROM) coupled to the memory array, some portions of the memory array are externally accessible but not modifiable.

In reference to claims 19, 36:

Gray discloses that memory could be password protected (Col. 9, lines 21-28), which meets the limitation of wherein some portions or the memory array are not externally accessible and are not modifiable.

In reference to claims 27, 44:

Gray discloses that the verification unit provides cryptographic capabilities (Col. 6, lines 55-57), which meets the limitation of the read only memory (ROM) further comprises cryptographic software.

In reference to claim 30:

Gray discloses that the authenticating system (Figure 2, element 10) meets the limitation of the claimed "computing device". Furthermore, when considering the disclosure of Gray it is clear that the computer 12 and the verification unit 20 make up a singular device for the simple reason that the verification unit 12 draws its power from the computer 12 (Col. 4, lines 15-20), which meets the limitation of the memory is a memory subsystem within the computing device.

In reference to claim 41:

Gray discloses a non-volatile memory system coupled to the processing system wherein the non-volatile memory system is external to the processing system internal to the computing system (Figure 2).

7. Claims 14, 25, 31, 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gray, U.S. Patent No. 6,268,788, in view of Zuk, U.S. Patent No. 5,745,571, and further in view of Reddy, U.S. Patent No. 6,824,051. Referring to claims 14, 25, 31, 42, Gray discloses that the system shown in Figure 2 (element 10) is a traditional computer or workstation (Col. 4, lines 13-15). Gray does not disclose that the system is a mobile system such as a PDA, which utilizes baseband/rf technology. However, it would have been obvious to provide the access control system described in Gray in a PDA embodiment because Gray discloses that there is an increased need to provide protection to sensitive information stored within computers systems

(Col. 1, lines 19-37) and Reddy shows that PDAs are a reasonable form of computer system (Col. 6, lines 25-33).

8. Claims 29, 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gray, in view of Zuk, U.S. Patent No. 5,745,571 and further in view of Lohstroh et al, US patent 5768373.

In reference to claims 29, 46:

Gray fails to explicitly disclose the method of claim 1 wherein the step of storing an encrypted access code comprises the step of storing a hashed access code.

Lohstroh, paragraph 15 teaches

(15) The encryption/decryption algorithm performed by units 252 and 258 is symmetric. Thus, since K.sub.acc is supplied to encryption unit 252, K.sub.acc must also be supplied to decryption unit 258. Yet, as with other keys, if K.sub.acc is stored in plaintext form in non-volatile storage means, and sometime later an unauthorized person discovers the location of K.sub.acc, the security of data will be compromised as other encrypted keys will then become accessible. Therefore, access key K.sub.acc is supplied on line 232 to encrypting unit 234 which operates according to well-known symmetric encryption/decryption algorithms such as "Blowfish", which can generally be found in Bruce Schneier, Applied Cryptography (2d.Ed. 1995). The resulting

*encrypted signal *K.sub.acc1 * produced on line 236 is stored in storage region 238. The key signal that is applied to encrypting unit 234 on line 264 is K.sub.pwh and is produced by hashing unit 262 from a user-supplied password on line 261. "Hashing" is generally the using of an algorithm to take a variable size input and produce a unique fixed-length identifier representative of the original input (here, the user password). One hash algorithm, MD5, or message digest 5, is generally known in the art, and is suitable for hashing a user password. Other algorithms are also generally known and are also suitable for hashing a user password in accordance with the invention. Often hash functions are thought to take a large block of data and reduce it to a smaller block. However, because the user password can vary from a few characters to up to 99 bytes in one embodiment, hash function 262 may produce a larger or smaller block of data than a given input (the user password), but it will return a password hash (K.sub.pwh) of consistently fixed length. In one embodiment using the MD5 hash function, such fixed length is set to 16 bytes.*

Thus Lohstroh teaches an embodiment where an access key or "access code" is encrypted by first hashing it.

"The key signal that is applied to encrypting unit 234 on line 264 is K.sub.pwh and is produced by hashing unit 262 from a user-supplied password on line 261."

Lohstroh also teaches that the password can vary from a few characters up to 99 bytes, but after the hash, it will return a password hash of consistently fixed length.

It would have been obvious to one of ordinary skill in the art at the time of invention to use a hash as a step in a cryptographic process to encrypt the hash in order to reduce a variable length password into a fixed length, providing for greater password security by masking the length of and number of characters within the password.

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to BENJAMIN E. LANIER whose telephone number is (571)272-3805. The examiner can normally be reached on M-Th 7:00am-5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Benjamin E Lanier/
Primary Examiner, Art Unit 2432